Notice of Allowability	Application No.	Applicant(s)	
	09/942,633	BLACK ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/21/2005*.

2. ☒ The allowed claim(s) is/are *2-7,12-17,22-27 and 31-39*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☒ Other Claims as renumbered.

Allowable Subject Matter

1. Claims 2-7, 12-17, 22-27 and 31-39 are allowed.

2. The following is an examiner's statement of reasons for allowance:

The primary reasons for the allowance of the independent claims 31, 34 and 37 are the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior art is Porras et al. (6,321,338; hereinafter Porras). Porras disclose a method of network surveillance that includes receiving network packets handled by a network entity and building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets that monitors data transfers, errors, or network connections. The method may also include responding based on the determining whether the difference between a short-term statistical profile and a long-term statistical profile indicates suspicious network activity. However, this art fails to anticipate or render the following limitations:

"Claims 31 and 37: receiving, in the higher-level correlation server, a plurality of delta packets from a plurality of lower-level correlation servers that include the first correlation server, wherein each delta packet contains the respective delta severity for each group of the respective lower-level correlation server that has a non-zero delta severity;

performing a first mathematical operation on the plurality of delta packets to form a new delta packet;

if the higher-level correlation server is the top level of the hierarchy of correlation servers, performing a second mathematical operation on the new delta packet and a stored severity packet to form a new severity packet; and

if the higher-level correlation server is not the top level of the hierarchy of correlation servers, propagating the new delta packet to a higher-level correlation server."

"Claim 34: sixth instructions for receiving, in the higher-level correlation server, a plurality of delta packets from a plurality of lower-level correlation servers that include the first correlation server, wherein each delta packet contains the respective delta severity for each group of the respective lower-level correlation server that has a non-zero delta severity;

seventh instructions for performing a first mathematical operation on the plurality of delta packets to form a new delta packet;

if the higher-level correlation server is the top level of the hierarchy of correlation servers, eighth instructions for performing a second mathematical operation on the new delta packet and a stored severity packet to form a new severity packet; and

if the higher-level correlation server is not the top level of the hierarchy of correlation servers, ninth instructions for propagating the new delta packet to a higher-level correlation server."

3. The dependent claims 2-7, 12-17, 22-27, 32, 33, 35, 36, 38 and 39 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

December 5, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100